APPENDIX D: NMCI APPLICATION RULESET (REVISED)

30 Jun 2004

NMCI Ruleset is also posted on NADTF website
http://cno-n6.hq.navy.mil/navcio/leg_apps.htm

Ruleset Is A Reference	The NMCI Ruleset is designed to be a summary of the information contained in the Legacy Applications Transition Guide (LATG) and the NMCI Release Development and Deployment Guide (NRDDG). Should questions arise from the use of the Ruleset, the user should refer to the LATG or NRDDG, or contact the Navy Applications Data Base Task Force (NADTF) for clarification.

Ruleset	Rule Name	Rule Description	Owner Required Action	Status
Rule 1	Windows 2000 (W2K) Compatible	The candidate application is not compatible with the Windows 2000 operating system. It either will not run properly under Windows 2000 or it will interfere with the normal functionality of the operating system.	Waivers will not be considered for this Ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA and owning FAM to upgrade the application to Windows 2000 compatibility or it should be replaced by another that is Windows 2000 compliant. Once a compliant version is identified it will be submitted for NMCI testing and certification. Applications that cannot be corrected will be quarantined for no more than 6 months and then will be removed from the quarantine workstation. The application will then be removed from the rationalized list and archived in the ISF Tools Database. Echelon II commands will cancel the RFS and unlink the application from their UICs in the ISF Tools Database.	Fail
Rule 2	NMCI Group Policy Object (GPO) Compatible	The candidate application is not compatible with the Group Policy Object (GPO) security rules for the workstation. For instance, if the candidate application requires full control of the c:\winnt folder in	Waivers will not be considered for this Ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA, owning FAM, ISF, and NMCI DAA to correct the GPO failure. NETWARCOM and ISF will provide the technical data detailing cause of the failure. Once the GPO failure is resolved, the application will be re-tested. GPO Policy changes may	Fail

Ruleset	Rule Name	Rule Description	Owner Required Action	Status
		order to run, this violates NMCI enterprise policy governing connection to the NMCI network.	be requested from the NMCI DAA. Applications that cannot be corrected will be quarantined for no more than 6 months and then be removed from the quarantine workstation. If the application cannot be corrected, it must be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	
Rule 3	No Duplication of Gold Disk Software or Services	The candidate application or service duplicates the functionality of the NMCI Standard Seat Services ("Gold Disk") applications. (Example: Word 2000 replaces all versions of WordPerfect and other word processors. Windows Media Player, Real Player, and QuickTime replace all other audio/video players).	Claimant should discard the current application and use the application or service that exists on the Gold Disk. This application is not eligible for quarantine. Waiver requests may be submitted to the appropriate FAM through the DADMS Waiver Questionnaire. But approvals will only be given if Claimant can show degradation to the mission and can show that they cannot afford to upgrade to authorized NMCI software or services. If the waiver is not approved or if no waiver is submitted, the application must be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database	Kill Unless waiver authorized
Rule 4	Comply with DON/NMCI Boundary 1 and 2 Policies	The ISF and NMCI DAA have determined, through testing, that the candidate application is non-compliant with NMCI Boundary firewall policies (violation of B1/B2 Rulesets).	Claimant must resolve violation with the application POR/CDA, owning FAM, ISF, and NMCI DAA to determine how to correct the Boundary policy violation. Once the policy violation is resolved, the application will be re-tested. Waivers will not be considered for this Ruleset. Requests to operate a non-compliant system for B1 Firewall policy violations are managed by OPNAV and B2 policy changes are reviewed and managed by the NMCI DAA. B2	Fail

Ruleset	Rule Name	Rule Description	Owner Required Action	Status
			boundary issues may be resolved by moving servers into NMCI enclave. Applications that cannot be corrected will be quarantined for no more than 6 months and will then be removed from the quarantine workstation. These applications will then be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	
Rule 5	No Setup, Installation, Deinstall, Update and Auto update Tools or Utilities	The candidate application is actually a tool or utility used to load and remove applications. Since ISF conducts all application installation and removal in NMCI, these types of files will not be authorized in ISF Tools DB or on the Rationalized List. Examples include Setup, Install, Uninstall, Launch, Auto launch, Run, Auto Run, Updater, Auto Updater or other installation-type Applications.	ISF will not test this application and waivers will not be considered. These types of applications will be removed from tracking and the Legacy Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	Kill
Rule 6	No Games	The candidate application is a "game" as defined by PEO-IT, NAVY IO and the PMO, and is prohibited on the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine the game is required for mission accomplishment (Modeling, Simulation, or Training). The Claimant must submit a waiver request to the appropriate FAM through the DADMS Waiver Questionnaire. Applications already approved by the M&S and/or Training FAM will not require waivers If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy	Kill Unless waiver authorized

Ruleset	Rule Name	Rule Description	Owner Required Action	Status
			Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	
Rule 7	Restrictions on Freeware or Shareware	The candidate application is "Freeware" or "Shareware" as defined by PEO-IT, NAVY IO or the PMO, and significant restrictions are imposed for applications using shareware or freeware in the NMCI environment. Enterprise life cycle support and licensing issues accompany most "Freeware and Shareware" and are the responsibility of the CDA or sponsoring FAM.	The candidate application either employs “freeware and/or shareware” in the construct of a GOTS application or is a “freeware and/or shareware” application which is sponsored by a CDA or a FAM. Enterprise life cycle support and licensing must be provided by the responsible CDA or the responsible FAM prior to the submission of freeware/shareware for NMCI testing. Waivers for freeware and shareware must be submitted by the POR/CDA or FAM and be approved by the NADTF prior to NMCI testing using the DADMS Waiver Questionnaire. The waiver request must include the CDAs/FAMs commitment for enterprise lifecycle and licensing support. The NADTF will coordinate the waiver request with the NMCI DAA. Freeware/shareware applications will not be installed on quarantine networks and/or dual desktop configurations. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy Applications Rationalized List and archived in the ISF Tools database. The Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	Kill Unless waiver authorized
Rule 8	No Beta/Test Software (Authorized on S&T Seats Only)	The candidate application is a "beta" or a "test" version, as defined by the PEO-IT, NAVY IO, or the PMO, and is therefore	ISF will not test this application and a waiver will not be considered. These types of applications will not be tracked through the Legacy Application Transition process. These applications are not entered into the ISF Tools	Kill

Ruleset	Rule Name	Rule Description	Owner Required Action	Status
		prohibited in the NMCI environment.	Database and not included on any rationalized list, nor should an RFS be submitted. If the Beta or Test Software is critical for mission accomplishment, the Claimant may purchase an S&T Seat. This application will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	
Rule 9	No Application Development Software (Authorized on S&T Seats Only)	The candidate application is "application development" software, as defined by either PEO-IT, NAVY IO or the PMO, and therefore is not authorized on standard NMCI Seats. The candidate application would be permitted if operated on an NMCI ordered Science and Technology (S&T) Seat. Application Development Software will not be tracked on the Rationalized List in the ISF Tools Database nor submitted for certification.	ISF will not test this application and a waiver will not be considered. These types of applications will not be tracked through the Legacy Application Transition process. These applications are not entered into the ISF Tools Database and not included on any rationalized list, nor should an RFS be submitted. If the application development software is critical for mission accomplishment, the Claimant may purchase an S&T Seat, which allows for the installation of development software. This application will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	Kill

Ruleset	Rule Name	Rule Description	Owner Required Action	Status
Rule 10	No Agent Software	The candidate application is "agent" software, as defined by PEO-IT, NAVY IO or the PMO. Agents in the NMCI environment are controlled by ISF. No other candidate agents are allowed in the NMCI environment. Agents are code modules installed on client machines (or network devices) often used to poll, monitor, and collect system or network node performance data and send it to management consoles elsewhere on the network. These present a security risk to NMCI. Network monitoring and management are the responsibilities of the ISF.	These types of applications will be removed from tracking in the Legacy Applications Rationalized List and the ISF Tools Database. These applications will not be considered for waivers. No polling and monitoring of legacy networks and systems and collecting of data is authorized from within NMCI Polling, monitoring and collecting system and network data from legacy networks and systems is still authorized from legacy network assets only. Viewing collected legacy network or system data from NMCI seats is allowed using non-agent software.	Kill
Rule 11	Gold Disk Compatible	The application software is not compatible with the standard "Gold Disk" software and services. This means that the candidate application does not interact properly with one or more of the set of applications or services that have been selected to be installed on all NMCI seats.	Waivers will not be considered for this Ruleset. The application is quarantined for no more than 6 months and then it is removed from the quarantine workstation. The application will be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel the RFS and unlink this application from their UICs in the ISF Tools database. Claimants and POR/CDA must work with the ISF to determine Gold Disk compatibility issues. The POR/CDA then works with the owning FAM to upgrade, replace, or retire the application. Once a compliant version is identified it must be submitted for NMCI testing.	Fail

Ruleset	Rule Name	Rule Description	Owner Required Action	Status
Rule 12	No Peripherals, Peripheral Drivers or Internal Hardware	The candidate submission is a component (driver or hardware helper app) dealing directly with allowing a peripheral piece of hardware to function (Scanner, Printer, Plotters, Chartmakers, CDRW drive, ZIP or JAZ drive, Camcorder, PDA, etc). This enabling software must be tracked with the hardware on the Peripherals list and not entered into ISF Tools Database or listed on the Rationalized List. Internal hardware and the associated driver are not permitted within NMCI.	Peripherals and enabling software (drivers) are not entered into the ISF Tools Database nor placed on the Rationalized List. Peripherals and Peripheral Drivers are tracked separately from the ISF Tools Database and the Rationalized List, and are included in the Peripheral Drivers List. The Peripheral Drivers List is submitted to the ISF on-site for processing. If the driver is part of a bundled software package, that bundled package is handled like an application. The bundled package is entered into the ISF Tools Database, placed on the Rationalized List, and tested by the ISF.	Kill
Rule 13	No personal, non-mission, or non-business related software	The candidate application is “personal, non-mission, or non-business related”, and is therefore prohibited in the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine that this application is required for mission accomplishment. These applications will not be installed on a quarantine workstation. The claimant must submit a waiver request to the appropriate FAM through the DADMS Waiver Questionnaire. If the waiver is not approved or submitted, the application must be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	Kill Unless waiver authorized

Ruleset	Rule Name	Rule Description	Owner Required Action	Status
Rule 14	8/16-Bit Applications	8-bit and 16-bit applications may migrate into the NMCI environment with an approved FAM waiver and a realistic migration plan that identifies a path to 32-bit status. Applications without approved waivers will not migrate to NMCI or Quarantined environments. Identification of an application as 8-bit or 16-bit does not stop the testing process (PIAB and LADRA). The application must pass all other rules and testing for 8-bit and 16-bit waivers to be approved.	Claimant and/or POR/CDA will submit a waiver immediately to the appropriate FAM through the DADMS Waiver Questionnaire requesting the 8/16-bit application migrate into NMCI. The request must include a detailed migration plan to get 8/16-bit application to 32-bit or web application status. ISF must process and certify the application while the waiver is being submitted. ISF will deploy the application while the waiver is being processed. If the waiver is not authorized (disapproved), the application is quarantined for no more than 6 months, then removed from the quarantine workstation and archived in the ISF Tools database. Applications for which a waiver was not submitted will not be quarantined, and will be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	Process and certify application Deployment while Waiver is authorized

Definition	
Fail	Fail is defined as violating the NMCI Application Ruleset by failing to successfully meet compliance or usability testing standards. These applications are flagged as Quarantined and will operate on a quarantined workstation in the legacy environment until the Ruleset violation or test failure is resolved or a waiver to operate within NMCI has been submitted and approved.
Kill	Kill is defined as violating the NMCI Application Ruleset. The application is not compliant with the rules and standards for applications within NMCI as set by the Navy IO. These applications will not be flagged as Quarantined and will be removed from the Rationalization List and ISF Tools database, unless a waiver to the rule is submitted and approved.
Application Development Software	Any software that generates or allows the user to create programming code which compiles into executable (.exe) files that are installed and can be run from the user's workstation. Application Development Software is only permitted to reside on S&T seats.
Agent Software	Any software that polls, monitors and/or captures network traffic or queries network nodes for the purpose of reporting the captured information back to the user or another network node. This type of information is considered sensitive and its capture and dissemination poses a security risk.